CLAIMS

1. A method for satisfiability (SAT) testing, given a set of formulas describing a target system, the formulas including clauses that include variables and express constraints on states of the system, the set of the formulas including at least a first and a second formula, the method comprising:

analyzing the first formula so as to deduce one or more conflict clauses, each such conflict clause expressing assignments of the variables that prevent a respective conflict, subject to which the first formula cannot be satisfied, while determining, for each of the conflict clauses, the clauses in the first formula that lead to the respective conflict;

identifying the conflict clauses for which the clauses that lead to the respective conflict in the first formula are a subset of the clauses in the second formula; and

analyzing the second formula subject to the identified conflict clauses, in order to determine whether the second formula can be satisfied.

2. A method according to claim 1, wherein the clauses are formulated in a conjunctive normal form (CNF), and wherein analyzing the second formula comprises forming a conjunction of the CNF of the second formula with the identified conflict clauses, and solving the conjunction.

3. A method according to claim 1, wherein analyzing the first formula comprises determining while analyzing the first formula whether, for each of the conflict clauses, the clauses that lead to the respective conflict are in the subset of the clauses in the second formula.

4. A method according to claim 1, wherein the set of formulas comprises a sequence of bounded model checking (BMC) instances, and wherein analyzing the first and second formulas comprises solving the BMC instances.

5. A method for bounded model checking (BMC) of a target system, comprising:

generating a succession of BMC instances describing the target system in the form of propositional satisfiability (SAT) formulas, the formulas comprising clauses that comprise variables and express constraints on states of the system;

analyzing a first instance in the succession of the BMC instances while deriving one or more conflict clauses that forbid certain assignments of the variables that give rise to conflicts, subject to which the first instance cannot be satisfied;

for each of the instances in the succession subsequent to the first instance, identifying the conflict clauses derived in a preceding one of the instances that are also pertinent to the subsequent instance; and

solving the subsequent instance subject to the identified conflict clauses, so as to seek a satisfying assignment of the variables, such that when a satisfying assignment is not found at the subsequent instance, one or more further conflict clauses are derived for use in solving a further one of the instances in the sequence.

6. A method according to claim 5, wherein identifying the conflict clauses comprises finding the conflict clauses that are induced by the clauses in the preceding

one of the instances that are also comprised in the subsequent instance.

7. A method according to claim 5, wherein solving the subsequent instance comprises solving the subsequent instance subject to substantially all of the conflict clauses identified as pertinent to the subsequent instance in a plurality of the instances in the sequence prior to the subsequent instance.

8. A method according to claim 5, wherein generating the succession of BMC instances comprises defining a model and a safety property of the target system, and wherein solving each of the instances comprises finding a violation of the safety property corresponding to the satisfying assignment.

9. A method according to claim 5, wherein generating the succession of BMC instances comprises formulating the logical clauses in a conjunctive normal form (CNF), and wherein solving the subsequent instance comprises forming a conjunction of the CNF of the subsequent instance with the identified conflict clauses, and solving the conjunction.

10. Apparatus for satisfiability (SAT) testing, comprising a satisfiability processor, which is arranged to receive a set of formulas describing a target system, the formulas comprising clauses that comprise variables and express constraints on states of the system, the set of the formulas comprising at least a first and a second formula, the processor being further arranged to analyze the first formula while deducing one or more conflict clauses, each such conflict clause prevent assignments

of the variables that give rise to a respective conflict, subject to which the first formula cannot be satisfied, while determining, for each of the conflict clauses, the clauses in the first formula that lead to the respective conflict, and to identify the conflict clauses for which the clauses that lead to the respective conflict in the first formula are a subset of the clauses in the second formula, the processor being still further arranged to analyze the second formula subject to the identified conflict clauses, in order to determine whether the second formula can be satisfied.

11. Apparatus according to claim 10, wherein the set of formulas are provided in a conjunctive normal form (CNF), and wherein the processor is arranged to analyze the second formula by forming a conjunction of the CNF of the second formula with the identified conflict clauses, and solving the conjunction.

12. Apparatus according to claim 10, wherein the processor is arranged to determine while analyzing the first formula whether, for each of the conflict clauses, the clauses that lead to the respective conflict are in the subset of the clauses in the second formula.

13. Apparatus according to claim 10, wherein the set of formulas comprises a sequence of bounded model checking (BMC) instances.

14. Apparatus for bounded model checking (BMC) of a target system, comprising a verification processor, which is arranged to receive a succession of BMC instances describing the target system in the form of propositional satisfiability (SAT) formulas, the formulas comprising

clauses that comprise variables and express constraints on states of the system, the processor being further arranged to analyze a first instance in the succession of the BMC instances while deriving one or more conflict clauses that forbid certain assignments of the variables that give rise to conflicts, subject to which the first instance cannot be satisfied, and to identify, for each of the instances in the succession subsequent to the first instance, the conflict clauses derived in a preceding one of the instances that are also pertinent to the subsequent instance, the processor being still further arranged to solve the subsequent instance subject to the identified conflict clauses, so as to seek a satisfying assignment of the variables, such that when a satisfying assignment is not found at the subsequent instance, the processor derives one or more further conflict clauses for use in solving a further one of the instances in the sequence.

15. Apparatus according to claim 14, wherein the processor is arranged to identify the conflict clauses that are also pertinent to the subsequent instance by finding the conflict clauses that are induced by the clauses in the preceding one of the instances that are also comprised in the subsequent instance.

16. Apparatus according to claim 14, wherein the processor is arranged to solve the subsequent instance subject to substantially all of the conflict clauses identified as pertinent to the subsequent instance in a plurality of the instances in the sequence prior to the subsequent instance.

17. Apparatus according to claim 14, wherein the succession of BMC instances are defined by a model and a safety property of the target system, and wherein the processor is arranged, by solving each of the instances, to find a violation of the safety property corresponding to the satisfying assignment.

18. Apparatus according to claim 14, wherein the succession of BMC instances are formulated in a conjunctive normal form (CNF), and wherein the processor is arranged to solve the subsequent instance by forming a conjunction of the CNF of the subsequent instance with the identified conflict clauses, and solving the conjunction.

19. A computer software product for satisfiability (SAT) testing, comprising a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to receive a set of formulas describing a target system, the formulas comprising clauses that comprise variables and express constraints on states of the system, the set of the formulas comprising at least a first and a second formula, and which instructions further cause the computer to analyze the first formula while deducing one or more conflict clauses, each such conflict clause expressing assignments of the variables that prevent a respective conflict, subject to which the first formula cannot be satisfied, while determining, for each of the conflict clauses, the clauses in the first formula that lead to the respective conflict, and to identify the conflict clauses for which the clauses that lead to the respective conflict in the first formula are a subset of

the clauses in the second formula, and to analyze the second formula subject to the identified conflict clauses, in order to determine whether the second formula can be satisfied.

20. A product according to claim 19, wherein the set of formulas are provided in a conjunctive normal form (CNF), and wherein the instructions cause the computer to analyze the second formula by forming a conjunction of the CNF of the second formula with the identified conflict clauses, and solving the conjunction.

21. A product according to claim 19, wherein the instructions cause the computer to determine while analyzing the first formula whether, for each of the conflict clauses, the clauses that lead to the respective conflict are in the subset of the clauses in the second formula.

22. A product according to claim 19, wherein the set of formulas comprises a sequence of bounded model checking (BMC) instances.

23. A computer software product for bounded model checking (BMC) of a target system, comprising a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to receive a succession of BMC instances describing the target system in the form of propositional satisfiability (SAT) formulas, the formulas comprising clauses that comprise variables and express constraints on states of the system, and further cause the computer to analyze a first instance in the succession of the BMC instances while deriving one or

more conflict clauses that forbid certain assignments of the variables that give rise to conflicts, subject to which the first instance cannot be satisfied, and to identify, for each of the instances in the succession subsequent to the first instance, the conflict clauses derived in a preceding one of the instances that are also pertinent to the subsequent instance, and which still further cause the computer to solve the subsequent instance subject to the identified conflict clauses, so as to seek a satisfying assignment of the variables, such that when a satisfying assignment is not found at the subsequent instance, the computer derives one or more further conflict clauses for use in solving a further one of the instances in the sequence.

24. A product according to claim 23, wherein the instructions cause the computer to identify the conflict clauses that are also pertinent to the subsequent instance by finding the conflict clauses that are induced by the clauses in the preceding one of the instances that are also comprised in the subsequent instance.

25. A product according to claim 23, wherein the instructions cause the computer to solve the subsequent instance subject to substantially all of the conflict clauses identified as pertinent to the subsequent instance in a plurality of the instances in the sequence prior to the subsequent instance.

26. A product according to claim 23, wherein the succession of BMC instances are defined by a model and a safety property of the target system, and wherein the instructions cause the computer, by solving each of the

instances, to find a violation of the safety property corresponding to the satisfying assignment.

27. A product according to claim 23, wherein the succession of BMC instances are formulated in a conjunctive normal form (CNF), and wherein the instructions cause the computer to solve the subsequent instance by forming a conjunction of the CNF of the subsequent instance with the identified conflict clauses, and solving the conjunction.